REALIZING RATIONAL REPRESENTATIONS IN MORDELL-WEIL GROUPS

BO-HAE IM AND MICHAEL LARSEN

Abstract. Let G be a finite group and V a finite-dimensional rational G-representation. We ask whether there exists a finite Galois extension L/K of number fields with Galois group G, an elliptic curve E/K, and a G-submodule of $E(L) \otimes \mathbb{Q}$ isomorphic to V.

1. Introduction

Let L/K be a Galois extension of number fields with group G. Let A/K be an abelian variety. We regard $A(L) \otimes \mathbb{Q}$ as a $\mathbb{Q}[G]$-module. We say that a faithful, irreducible, rational representation V of a finite group G is *Mordell-Weil*, or more specifically, *Mordell-Weil in dimension* $\dim A$ or *Mordell-Weil over K in dimension* $\dim A$, if V arises as a G-submodule of $A(L) \otimes \mathbb{Q}$ for some triple (K, L, A). It turns out that every rational irreducible representation of a finite group is Mordell-Weil:

Theorem 1.1. *If G is a finite group, V is a finite-dimensional $\mathbb{Q}$-vector space and $\rho : G \hookrightarrow \mathrm{Aut}(V)$ is a faithful irreducible rational representation, then there exists a finite Galois extension of number fields, L/K, an isomorphism $\mathrm{Gal}(L/K) \to G$, and a $\mathrm{Gal}(L/K)$-stable subspace W of $A(L) \otimes \mathbb{Q}$ such that by transport of structure, W is isomorphic to V as a $\mathbb{Q}[G]$-module.*

We are particularly interested in the case $\dim A = 1$, and we present two methods, one geometric, and one arithmetic, for showing that certain interesting pairs (G, V) can be realized inside the Mordell-Weil groups of elliptic curves. These two methods are loosely analogous to two established approaches to the inverse Galois problem, namely the rigidity method, and the use of automorphic forms.

Date: February 1, 2010.

2000 *Mathematics Subject Classification.* 12E30.

Michael Larsen was partially supported by NSF grants DMS-0100537 and DMS-0800705.

2. Hilbert Irreducibility

The geometric method of realizing a pair (G, V) was inspired by [Im]. The idea is to look for a diagram

$$\begin{array}{ccc} X & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \longrightarrow & A/G \end{array}$$

over a number field K. Here, the first row consists of a G-equivariant map from a curve to an abelian variety and the vertical arrows are quotient maps. Hilbert irreducibility gives a K-point in $\mathbb{P}^1 = X/G$ whose preimage in X consists of a single point Spec L, where $G = \mathrm{Gal}(L/K)$. This point generates a $\mathbb{Q}[G]$-submodule of $A(L) \otimes \mathbb{Q}$; the only difficulty is to insure that this module contains V as a submodule. This can be achieved by the following proposition:

Proposition 2.1. *Let A/K and B/K be abelian varieties and G a finite group of K-automorphisms of A. Suppose A contains an irreducible curve X which is stabilized by G and is not contained in the translate of any proper abelian subvariety of A. Let V denote any $\mathbb{Q}$-irreducible subrepresentation of $\mathrm{Hom}_K(A, B) \otimes \mathbb{Q}$. If X/G is a rational curve over K, then there exists a Galois extension L/K with group G and a $\mathbb{Q}[G]$-submodule of $B(L) \otimes \mathbb{Q}$ isomorphic to V. In particular, (G, V) is Mordell-Weil.*

Proof. Let v denote any non-zero vector in V and $\phi \in \mathrm{Hom}_K(A, B)$ a non-zero scalar multiple of v. Let $P = X/G$ and π the quotient morphism $X \to P$. For $g \neq 1$, X is not contained in the kernel of $1 - g$ acting on A. Therefore, the morphism $X \to P$ is a regular branched covering with Galois group G. By an observation of Silverman [Si], originally made in the setting of elliptic curves, but equally valid for abelian varieties, the set of torsion points on B which are defined over number fields of degree $\leq |G|$ over K is finite. Therefore, the set of $p \in P(K)$ such that $\pi^{-1}(p) \cap \phi^{-1}B(\bar{K})_{\mathrm{tor}} \neq \emptyset$ is finite. By the Hilbert irreducibility theorem, there exists $x \in X(\bar{K})$ such that $\pi(x) \in P(K)$, the $\mathrm{Gal}(\bar{K}/K)$-orbit of x coincides with the G-orbit of x, and $\phi(x)$ is a point of infinite order on B.

Evaluation at x gives a $\mathbb{Q}[G]$-linear map $\mathrm{Hom}_K(A, B) \otimes \mathbb{Q} \to B(L) \otimes \mathbb{Q}$. As composition with the inclusion $V \hookrightarrow \mathrm{Hom}_K(A, B) \otimes \mathbb{Q}$ is non-zero, $B(L) \otimes \mathbb{Q}$ contains at least one copy of V. □

Given a finite group G, an n-tuple $\mathbf{g} = (g_1, \ldots, g_n) \in G^n$ satisfying

$$g_1 g_2 \cdots g_n = 1,$$

and an n-tuple $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{P}^1(\overline{\mathbb{Q}})^n$ whose coordinates are pairwise distinct, we define $U_{\mathbf{g},\mathbf{p}}/\mathbb{C}$ as the open curve such that $U_{\mathbf{g},\mathbf{p}}(\mathbb{C})$ is the regular covering space of $\mathbb{P}^1(\mathbb{C}) \setminus \{p_1, \ldots, p_n\}$ with deck transformations in $\langle g_1, \ldots, g_n \rangle$ and local monodromy g_i at p_i. We assume $G = \langle g_1, \ldots, g_n \rangle$, so

G acts freely on $U_{\mathbf{g},\mathbf{p}}$. Let $X_{\mathbf{g},\mathbf{p}}$ denote the non-singular compactification of $U_{\mathbf{g},\mathbf{p}}$. The action of G on $U_{\mathbf{g},\mathbf{p}}$ extends to $X_{\mathbf{g},\mathbf{p}}$, and $\mathbb{P}^1 = X_{\mathbf{g},\mathbf{p}}/G$. Moreover, $X_{\mathbf{g},\mathbf{p}}$ can be defined over some number field.

By a theorem of Weil [Se, VI Prop. 7], the representation of G on $H^1(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q})$ satisfies

$$H^1(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q}) \oplus I_G \oplus I_G \cong \bigoplus_{i=1}^{n} \mathrm{Ind}_{\langle g_i \rangle}^{G} I_{\langle g_i \rangle}. \tag{1}$$

An immediate consequence of this is that for any complex representation $V_{\mathbb{C}}$ of G,

$$2\dim V_{\mathbb{C}} - 2\dim V_{\mathbb{C}}^{G} \leq \sum_{i=1}^{n} \dim V_{\mathbb{C}} - \dim V_{\mathbb{C}}^{g_i}.$$

This is the finite case of a well-known result of L. Scott [Sc]. We are interested in the case $V_{\mathbb{C}} = V \otimes_{\mathbb{Q}} \mathbb{C}$, where V is a $\mathbb{Q}$-vector space on which G acts. Here we have the following:

Proposition 2.2. *If V is a rational representation, then*

$$-2\dim V + 2\dim V^{G} + \sum_{i=1}^{n} \dim V - \dim V^{g_i} = 2g \tag{2}$$

for some non-negative integer g.

Proof. The space

$$W = \mathrm{Hom}_G(H^1_{\mathrm{sing}}(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q}), V)$$

inherits a rational Hodge structure of weight 1 from $H^1_{\mathrm{sing}}(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q})$ and is therefore of even dimension; on the other hand, its dimension is given by the left hand side of (2).

□

We call g the *genus* of the triple $(G, V, \mathbf{g})$. We can now prove a more precise version of Theorem 1.1.

Theorem 2.3. *Let $(G, V, \mathbf{g})$ is a triple consisting of a finite group, an irreducible rational representation space, and a generating n-tuple with product 1 such that $(G, V, \mathbf{g})$ has genus $g > 0$. Then (G, V) is Mordell-Weil in dimension g, i.e., there exists a number field K, an abelian variety A/K of dimension g, a Galois extension L/K, an isomorphism $\mathrm{Gal}(L/K) \to G$, and a $\mathrm{Gal}(L/K)$-stable subspace W of $A(L) \otimes \mathbb{Q}$ such that by transport of structure, W is isomorphic to V as $\mathbb{Q}[G]$-module.*

Proof. Let v denote a non-zero vector in the representation space V, and let $\Lambda = \mathbb{Z}[G]v$ denote the corresponding lattice. If A/K is an abelian variety with a G-action, we define $A_\Lambda := A \otimes_{\mathbb{Z}[G]} \Lambda$ to be the functor represented by $S \mapsto A(S) \otimes_{\mathbb{Z}[G]} \Lambda$ for every scheme S over K. Concretely, A_Λ is the quotient of A by $\sum \alpha A$, where the sum is taken over $\alpha \in \ker(\mathbb{Z}[G] \to \Lambda)$. As the quotient of an abelian variety by a closed subgroup, A_Λ is

again an abelian variety. Its Lie algebra is $\mathrm{Lie}(A) \otimes_{\mathbb{Q}[G]} V_{\mathbb{Q}}$. The vector space $\mathrm{Hom}_K(A, A_\Lambda) \otimes \mathbb{Q}$ admits a G-action (given by the action of G on A) and contains a non-zero vector e (the natural quotient map) provided that $\mathrm{Lie}(A) \otimes_{\mathbb{Q}[G]} V_{\mathbb{Q}}$, and therefore A_Λ, is non-zero. On the other hand, e is annihilated by $\ker(\mathbb{Z}[G] \to \Lambda)$. It follows that $\mathbb{Q}[G]e \cong V$ as $\mathbb{Q}[G]$-module.

Fix $\mathbf{p} \in \mathbb{P}^1(\overline{\mathbb{Q}})^n$. Let D denote the divisor of $X_{\mathbf{g},\mathbf{p}}$ which is the inverse image under the map $X_{\mathbf{g},\mathbf{p}}$ of the divisor $[0]$ on $\mathbb{P}^1$. Let J denote the Jacobian variety of $X_{\mathbf{g},\mathbf{p}}$. By hypothesis,

$$\begin{aligned}\dim J_\Lambda = \frac{\dim \mathrm{Lie}(J) \otimes_{\mathbb{Q}[G]} V_{\mathbb{Q}}}{2} &= \frac{\dim H^1_{\mathrm{sing}}(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q})^* \otimes_{\mathbb{Q}[G]} V}{2} \\ &= \frac{\dim H^1_{\mathrm{sing}}(X_{\mathbf{g},\mathbf{p}}(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}[G]} V}{2} = g > 0.\end{aligned}$$

The morphism $X_{\mathbf{g},\mathbf{p}} \to J$ given by $Q \mapsto |G|[Q] - D$ is G-equivariant, and the quotient $X_{\mathbf{g},\mathbf{p}}/G$ is isomorphic to $\mathbb{P}^1$. The theorem follows by applying Proposition 2.1 to the morphism $J \to J_\Lambda$.

□

We remark that the Hilbert irreducibility argument actually gives a little more: it shows that we may choose infinitely many linearly disjoint extensions L_i over K, all with Galois group G and submodules $V_i \subset A(L_i)$ which are isomorphic to V as $\mathrm{Gal}(L_i/K) = G$-modules.

3. Some genus 1 triples

Proposition 3.1. *Let G be the Weyl group of an irreducible root system of rank r and V its reflection representation. Let $G^\circ = G \cap \mathrm{SO}(V)$. Then there exist vectors $\mathbf{g} \in G^{2r+2}$ and $\mathbf{g}^\circ \in (G^\circ)^{r+1}$ such that $(G, V, \mathbf{g})$ and $(G^\circ, V, \mathbf{g}^\circ)$ have genus 1.*

Proof. Let $s_1, \dots, s_r$ denote the simple reflections. We can take

$$\mathbf{g} = (s_1, s_1, s_2, s_2, \dots, s_r, s_r, s_1, s_1).$$

As $\dim V^{s_i} = r - 1$, we have $g = 1$. Every Dynkin diagram with $r - 1 \geq 2$ edges can be written as the union of two paths which meet at a single vertex: $i_1, \dots, i_p$ and $j_1, \dots, j_q$, with $p + q = r + 1$. Then we can take

$$\mathbf{g}^\circ = (s_{i_1} s_{i_2}, s_{i_2} s_{i_3}, \dots, s_{i_p} s_{i_1}, s_{j_1} s_{j_2}, s_{j_2} s_{j_3}, \dots, s_{j_q} s_{j_1}).$$

Every product of the form $s_{i_m} s_{i_n}$ or the form $s_{j_m} s_{j_n}$ is obviously in the group $\langle \mathbf{g}^\circ \rangle$ generated by the coordinates of $\mathbf{g}^\circ$, and as there exists one vertex of the form $i_k = j_l$, every product $s_{i_m} s_{j_n} = s_{i_m} s_{i_k} s_{j_l} s_{j_n}$ is again in $\langle \mathbf{g}^\circ \rangle$. It follows that this group is the kernel of the determinant map on G. Each product of two simple reflections fixes a subspace of V of codimension 2, so again $g = 1$. □

Proposition 3.2. *If G is the automorphism group $2.\mathrm{Co}_1$ of the Leech lattice Λ_{24} and $V = \Lambda_{24} \otimes \mathbb{Q}$, then there exists $\mathbf{g} \in G^3$ such that $(G, V, \mathbf{g})$ has genus 1.*

Proof. By [DA], Co_1 has a $(2A, 7B, 13A)$ generation, and this can be lifted to a generating triple $(\widetilde{2\mathrm{A}}, \widetilde{7\mathrm{B}}, -\widetilde{13\mathrm{A}})$ in $2.\mathrm{Co}_1$, where the lifts $\widetilde{7\mathrm{B}}$ and $\widetilde{13\mathrm{A}}$ are chosen to have order 7 and 13 respectively; the lift of 2A is then determined by the product 1 condition. By [Atlas], the resulting triple has genus 1. □

There is an extensive literature devoted to pairs of elements (g_1, g_2) generating sporadic simple groups G. In particular, cases in which the orders of g_1, g_2, and g_1g_2 are all low have been extensively studied, in an attempt to classify simple Hurwitz groups and, more generally, to compute the symmetric genera of sporadic groups. Any generating pair (g_1, g_2) gives rise to a triple $\mathbf{g} = (g_1, g_2, g_2^{-1}g_1^{-1})$ as above. The following table, giving some examples of genus 1, is mainly extracted from this literature.

Group	Character	Dimension	Generators	Reference
M_{11}	χ_2	10	see (M_{11})	
M_{12}	χ_2	11	see (M_{12})	
M_{22}	χ_2	21	see (M_{22})	
M_{23}	χ_2	22	see (M_{23})	
HS	χ_2	22	2B, 5B, 7A	[GM2]
McL	χ_2	22	2A, 5A, 8A	[CWW]
M_{24}	χ_2	23	see (M_{24})	
Co_3	χ_2	23	2B, 3C, 11A	[GM1]
Co_2	χ_2	23	2B, 5A, 11A	[GM3]
$2.\mathrm{Co}_1$	χ_{102}	24	$\widetilde{2\mathrm{A}}$, $\widetilde{7\mathrm{B}}$, $-\widetilde{13\mathrm{A}}$	[DA]
Tits	χ_6	78	2A, 3A, 13A	[AI]
J_2	χ_{12}	160	2B, 3B, 7A	[Wo]

Where no reference is given, the assertions can easily be checked by machine, e.g., using [GAP]. Using [Atlas] notation (except that for the large Mathieu groups we write $A, B, C, \ldots, X$ instead of $0, 1, \ldots, 22, \infty$), we have generating pairs as follows:

(M_{11}) $\quad (0183649X257)\ (07365481)(29) = (2X)(34)(59)(67)$

(M_{12})

$$(058263X4179)\ (0\infty92)(13)(458X)(67) = (0\infty)(1X)(25)(37)(48)(69)$$

(M_{22})

$$(\mathtt{AFMIHBLCRPD})(\mathtt{EGSVQJNOUKT})\ (\mathtt{ADLQF})(\mathtt{BHMVJ})(\mathtt{CPTUO})(\mathtt{ERNSG})$$
$$=(\mathtt{CD})(\mathtt{EP})(\mathtt{HI})(\mathtt{JL})(\mathtt{KT})(\mathtt{MQ})(\mathtt{NV})(\mathtt{OR})$$

(M_{23})

$$(\mathtt{AWEIHURTPBCSLGMOKJVNFD})\ (\mathtt{ADBPW})(\mathtt{CFNJS})(\mathtt{ETOUH})(\mathtt{GLKRQ})$$
$$=(\mathtt{CD})(\mathtt{EP})(\mathtt{HI})(\mathtt{JL})(\mathtt{KT})(\mathtt{MQ})(\mathtt{NV})(\mathtt{OR})$$

(M_{24})

$$(\mathtt{ATSX})(\mathtt{DW})(\mathtt{EQIG})(\mathtt{FULV})(\mathtt{HJOM})(\mathtt{NP})\ (\mathtt{ASJVOTIFHPWBDNMLCUQKERG})$$
$$=(\mathtt{AX})(\mathtt{BW})(\mathtt{CL})(\mathtt{DP})(\mathtt{ER})(\mathtt{FJ})(\mathtt{GT})(\mathtt{HN})(\mathtt{IU})(\mathtt{KQ})(\mathtt{MV})(\mathtt{OS})$$

4. Modular curves and Steinberg representations

If n is a positive integer, we define as usual

$$\Gamma(n) := \ker \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$$

and

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{n} \right\}.$$

Let

$$\Gamma_{m,n} := \Gamma(m) \cap \Gamma_0(n).$$

Thus $\Gamma_{m,n}$ is normal in $\Gamma_0(n)$, and there is a natural inclusion homomorphism

$$\Gamma_0(n)/\Gamma_{m,n} \to \mathrm{SL}_2(\mathbb{Z})/\Gamma(m) \cong \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}).$$

If m and n are relatively prime, this inclusion is an isomorphism, by the Chinese remainder theorem. Let $Y_0(n)$ and $Y_{m,n}$ denote the quotient of the upper half-plane by $\Gamma_0(n)$ and $\Gamma_{m,n}$ respectively. If $(m,n) = 1$, $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ acts faithfully on $Y_{m,n}$ with quotient $Y_0(n)$. Letting $X_0(n)$ (resp. $X_{m,n}$) denote the non-singular compactification of $Y_0(n)$ (resp. $Y_{m,n}$), the $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$-action on $Y_{m,n}$ extends uniquely to $X_{m,n}$, and the quotient is $X_0(n)$.

Theorem 4.1. *If there exists an elliptic curve of conductor pN where p is prime, N is relatively prime to p, and $X_0(N)$ has genus 0, then the Steinberg representation of $\mathrm{SL}_2(\mathbb{F}_p)$ is Mordell-Weil in dimension 1.*

Proof. Let $J_{p,N}$ denote the Jacobian variety of $X_{p,N}$. We consider the diagram

$$\begin{array}{ccc} X_{p,N} & \longrightarrow & J_{p,N} \\ \downarrow & & \downarrow \\ X_0(N) & \longrightarrow & J_{p,N}/\mathrm{SL}_2(\mathbb{F}_p). \end{array}$$

Let $A = J_{p,N}$ and $B = E$, where E is any elliptic curve of conductor Np. As $\Gamma_0(pN) \subset \Gamma_{p,N}$, $X_{p,N}$ maps onto $X_0(pN)$, which maps onto E by the modularity of elliptic curves over $\mathbb{Q}$. Let $\pi\colon A \to B$ be a non-constant map factoring through the Jacobian variety of $X_0(pN)$. Applying Proposition 2.1, it suffices to prove that $\mathrm{Hom}_{\mathbb{C}}(A,B) \otimes \mathbb{Q}$, regarded as a rational $\mathrm{SL}_2(\mathbb{F}_p)$ representation contains the Steinberg representation as a subrepresentation.

Let P denote the image of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{F}_p)$, i.e., the group of upper triangular matrices in $\mathrm{SL}_2(\mathbb{F}_p)$. By construction, π is fixed by the action of P on A. Thus, the $\mathbb{Q}[\mathrm{SL}_2(\mathbb{F}_p)]$-submodule of $\mathrm{Hom}_{\mathbb{C}}(A,B) \otimes \mathbb{Q}$ generated by π is a quotient of $\mathrm{Ind}_P^{\mathrm{SL}_2(\mathbb{F}_p)} \mathbb{Q}$, which is isomorphic to the direct sum of a trivial 1-dimensional representation and the Steinberg representation. We need only prove, therefore, that the action of of $\mathrm{SL}_2(\mathbb{F}_p)$ on π is non-trivial, i.e., that π does not factor through the maximal $\mathrm{SL}_2(\mathbb{F}_p)$-invariant quotient, $A_{\mathrm{SL}_2(\mathbb{F}_p)}$, of A. However,

$$H^1_{\mathrm{sing}}(A_{\mathrm{SL}_2(\mathbb{F}_p)}(\mathbb{C}), \mathbb{Q}) \cong H^1_{\mathrm{sing}}(A(\mathbb{C}), \mathbb{Q})_{\mathrm{SL}_2(\mathbb{F}_p)} \cong H^1_{\mathrm{sing}}(X_{p,N}(\mathbb{C}), \mathbb{Q})_{\mathrm{SL}_2(\mathbb{F}_p)},$$

which is trivial since the quotient of $X_{p,N}$ by $\mathrm{SL}_2(\mathbb{F}_p)$ is the genus 0 curve $X_0(N)$.

□

Corollary 4.2. *The Steinberg representation of* $\mathrm{SL}_2(\mathbb{F}_p)$ *is Mordell-Weil for all primes* $p < 1000$.

Proof. This follows immediately from the proposition by inspecting Cremona's tables [Cr].

□

We remark that it is expected but not yet known that infinitely many primes satisfy the hypotheses of Theorem 4.1. Work of Friedlander and Iwaniec [FI] gives some hope that this problem may be accessible.

We note that by restricting the Steinberg representation to the group $\mathbb{Z}/p\mathbb{Z}$ of unitriangular matrices in $\mathrm{SL}_2(\mathbb{Z}/\mathbb{Z})$, we deduce that the regular representation of $\mathbb{Z}/p\mathbb{Z}$ is Mordell-Weil in dimension 1 for all primes $p < 1000$. In fact, one can prove more:

Proposition 4.3. *For every prime* p*, the regular representation of* $\mathbb{Z}/p\mathbb{Z}$ *is Mordell-Weil in dimension* 1.

Proof. Mazur and Kurčanov observed [Ku], that under certain common conditions, the rank of an elliptic curve over a $\mathbb{Z}_p$-extension of a number field is infinite. For convenience, we use a more recent result due to Cornut [Co] and Vatsal [Va].

We fix a non-CM elliptic curve E with root number -1 and conductor $N < 1000$. We let K_∞ denote the anti-cyclotomic p-extension of $\mathbb{Q}(i)$. Every $p > 1000$ is prime to N and the conductor of E, and it follows that the rank of E over K_∞ is infinite. Therefore there exists an abelian p-extension K_{n+1}/K_n such that

$$\dim E(K_{n+1}) \otimes \mathbb{Q} > \dim E(K_n) \otimes \mathbb{Q} > 0,$$

and it follows that the $\mathrm{Gal}(K_{n+1}/K_n)$-module $E(K_{n+1}) \otimes \mathbb{Q}$ contains a copy of the regular representation of $\mathbb{Z}/p\mathbb{Z}$.

□

References

[AI] Ibrahim, Mohammed Ali Faya; Ali, Faryad: $(2, 3, t)$-generations of the Tits simple group ${}^2F_4(2)'$, preprint.

[Cr] Cremona, John: Elliptic curve data, (http://www.warwick.ac.uk/∼masgaj/ftp/data/INDEX.html).

[CWW] Conder, M. D. E.; Wilson, R. A.; Woldar, A. J.: The symmetric genus of sporadic groups. *Proc. Amer. Math. Soc.* **116** (1992), no. 3, 653–663.

[Atlas] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A.: *Atlas of finite groups.* Oxford University Press, Eynsham, 1985.

[Co] Cornut, Christophe: Mazur's conjecture on higher Heegner points. *Invent. Math.* **148** (2002), no. 3, 495–523.

[DA] Darafsheh, M. R.; Ashrafi, A. R.: $(2, p, q)$-generations of the Conway group Co_1. *Kumamoto J. Math.* **13** (2000), 1–20.

[FI] Friedlander, John Iwaniec, Henryk: The polynomial X^2+Y^4 captures its primes. *Ann. of Math. (2)* **148** (1998), no. 3, 945–1040.

[GM1] Ganief, Shahiem; Moori, Jamshid: (p, q, r)-generations of the smallest Conway group Co_3. *J. Algebra* **188** (1997), no. 2, 516–530.

[GM2] Ganief, Shahiem; Moori, Jamshid: (p, q, r)-generations and nX-complementary generations of the sporadic groups HS and McL. *J. Algebra* **188** (1997), no. 2, 531–546.

[GM3] Ganief, Shahiem; Moori, Jamshid: Generating pairs for the Conway groups Co_2 and Co_3, *J. Group Theory* **1** (1998), no. 3, 237–256.

[GAP] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.4.7; 2006, (http://www.gap-system.org).

[Im] Im, Bo-Hae: Mordell-Weil groups and the rank of elliptic-curves over large fields. *Canad. J. Math.* **58** (2006), no. 4, 796–819.

[Ku] Kurčanov, P. F.: Elliptic curves of finite rank over Γ-extensions. (Russian) *Mat. Sb. (N.S.)* **90(132)** (1973), 320–324, 327.

[Sc] Scott, Leonard L.: Matrices and cohomology. *Ann. of Math. (2)* **105** (1977), no. 3, 473–492.

[Se] Serre, Jean-Pierre: Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[Si] Silverman, Joseph: Integer points on curves of genus 1. *J. London Math. Soc. (2)* **28** (1983), no. 1, 1–7.

[Va] Special values of anticyclotomic L-functions. *Duke Math. J.* **116** (2003), no. 2, 219–261.

[Wo] Woldar, A. J.: On Hurwitz generation and genus actions of sporadic groups. *Illinois J. Math.* **33** (1989), no. 3, 416–437.

Department of Mathematics, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul, 155-756, South Korea

E-mail address: bohaeim@gmail.com

Department of Mathematics, Indiana University, Bloomington, Indiana 47405, USA

E-mail address: larsen@math.indiana.edu